- Document operational use of social media, including the date, site(s) accessed, information collected, and how it was used in the same manner that the Department would document information collected from any source in the normal course of business.

Rules of Behavior for Law Enforcement Use of Social Media

When utilizing social media for authorized law enforcement activities, situational awareness, or intelligence purposes, and adherence to the above-listed general rules would impede operational efficiency, the rules of behavior listed below must be followed. These rules have been adapted from the online investigative principles outlined in DOJ's 1999 Online Investigative Principles for Federal Law Enforcement Agents.

1. Obtaining Information from Unrestricted Sources.

   Obtain information from publicly accessible social media sources and facilities, including but not limited to Facebook, Twitter, MySpace, and blogs, under the same conditions that information from other sources generally open to the public may be obtained. This principle applies to publicly accessible sources located in foreign jurisdictions as well as those in the United States.

2. (b)(7)(E)

3. Real-Time Communications.

   Passively observe and log real-time electronic communications open to the public on social media sites, such as Facebook and Twitter, under the same circumstances in which a public meeting may be attended.

4. Accessing Restricted Sources.

   Do not access restricted social media sources or facilities absent legal authority permitting entry into private space.

5. Communicating Through Social Media Generally.

   Use social media to communicate in the same manner as other types of communication tools, such as the telephone and the mail, are used. The content of social media communications (e.g., a tweet, a Facebook wall post, an electronic message) should be retained in the same manner that paper communications are retained. Any electronic communication,

including social media communications, may be a Federal record and must be preserved accordingly.

6. [redacted]

7. [redacted]

8. (b)(6);(b)(7)(C)

9. [redacted]

10. International Issues.

Use reasonable efforts to ascertain whether any pertinent computer system, data, witness, or subject is located in a foreign jurisdiction, unless gathering information from social media facilities configured for public access. Whenever an item or person is located abroad,

follow Secret Service policies and procedures for international investigations.

II. Documenting Online Investigations.

Track the use of social media for law enforcement purposes in the same manner that actions taken in the physical world are documented. Balance the need for good record keeping practices with considerations against keeping voluminous irrelevant records and in accordance with Secret Service records retention policies.

These Rules of Behavior for General Operational and Law Enforcement Use of Social Media are not intended to, do not, and may not be relied upon to create any right or benefit, substantive or procedural, enforceable at law by any party in any administrative, civil, or criminal matter. Violation of these rules of behavior, however, may result in discipline.

All Secret Service employees and contractors are required to complete annual privacy training for the operational use of social media. Completion of this privacy training is a prerequisite for obtaining access to social media for operational purposes. Upon completion of this training, each employee and contractor must self certify that they have read and understood the Rules of Behavior. Employees and contractors who are granted such access must renew their access authority annually by taking refresher training and recertifying that they have read and understand the Rules of Behavior. The Secret Service Privacy Office will send an official message to all employees giving notification when the social media training is available on LMS. All employees and contractors must complete this training on the relevant policies regarding the operational use of social media by no later than March 1, 2013.

activities conducted by Secret Service personnel, or is provided to the Secret Service unsolicited. Secret Service personnel who are authorized and have access may enter the collected information directly into PTMS to update or complete a record. Users may also attach an electronic copy of the source record to the PTMS case record.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

USSS routinely collects publicly available information, to include social media, and information that may be obtained through commercially available Internet sources. USSS uses such tools for situational awareness regarding protected persons, events, or facilities, and to ascertain the location of subjects of investigations. This information may be used to develop preliminary leads.

2.4 Discuss how accuracy of the data is ensured.

The information is checked for accuracy during the course of the investigative process through personal interviews and again when information is entered into PTMS, when discrepancies may be detected. Typically, discrepancies are due to data entry errors. If discrepancies are found, protective intelligence personnel can correct the entry and update the information.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: Due to the inherent risk of inaccurate information from publicly available sources, such as social media, there is a risk that the Secret Service will incorrectly identify individuals as the subjects of protective threat assessments.

Mitigation: This risk is partially mitigated. Secret Service identifies information from third-party social media services submitted voluntarily by members of the public and compares that information with information available through a variety of public and government sources. By bringing together and comparing many different sources of information, Secret Service personnel attempt to provide a more accurate picture of potentially threatening activities. Requests to amend records will be considered on a case-by-case basis if made in writing to the Secret Service's FOIA/PA Officer, Communications Center (FOIA/PA), 245 Murray Lane, S.W., Building T-5, Washington, D.C. 20223.

Privacy Risk: There is a risk of over collection of information when the Secret Service collects publicly available information associated with a particular location or event to be visited/attended by a Secret Service protectee or otherwise secured by the Secret Service.

Mitigation: Data is most often collected by the Secret Service from other law enforcement

agencies or directly from the individual during the course of an investigation based on voluntary cooperation. Data may also be obtained lawfully from public or law enforcement records (e.g., existing PTMS or other agency records). Further, the Secret Services uses PII for the limited purpose of enabling positive identification so that (a) the individual is identifiable during future interactions with the agency; (b) the individual is not erroneously identified as, or linked to, another individual; and (c) further investigation can be conducted, if necessary.

Privacy Risk: There is a risk of inaccurate information because PTMS relies heavily on information from other government law enforcement databases and is generally not the original source of collection.

Mitigation: No action will be taken unless the information received has been reviewed by Secret Service employees engaged in protective activities who are trained in the interpretation of the information and familiar with the environment in which the information is collected and used. PTMS supports USSS personnel in identifying individuals known to the Secret Service or other U.S. Government agencies who may pose a risk of harm to protected persons, events, or facilities.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

The information is used to support the Secret Service in accomplishing its protective mission, specifically in development of threat assessments to assist in creating a secure environment for Secret Service protected persons, events, and facilities. A threat assessment offers a description of the current threat environment for those individuals or events protected by the Secret Service. Use of PTMS is restricted to personnel who need information to effectively perform their job functions. The Secret Service uses PTMS to identify individuals known to the Secret Service or other U.S. Government agencies who may pose a risk of harm to protected persons, events, or facilities.

Data is collected in order to assess an individual, group, or incident that may pose a threat or potential threat to Secret Service protected persons, events, or facilities. The results of such investigations and/or assessments are disseminated to internal Secret Service customers, including protective details, to support their protective efforts, and within the Department of Homeland Security.

~~LAW ENFORCEMENT SENSITIVE~~

Protective Intelligence and Assessment Division (PID)

Open Source Intelligence (OSINT) Program

Knowledge Transfer Document*

~~LAW ENFORCEMENT SENSITIVE~~

- This document supports the program needs of the Component Acquisition Executive to satisfy DHS requirements for project status reports and quad charts

Protective Intelligence and Assessment Division (PID) Open Source Intelligence (OSINT) Program

EXECUTIVE SUMMARY

The PID OSINT program is designed to provide real-time situational awareness and threat identification for protectee travel and investigative support for protective intelligence operations. The program comprises a cadre of trained OSINT analysts, who are assigned to the OSU unit and whose activities are conducted (b)(7)(E) Daily, the analysts provide OSINT monitoring for (b)(7)(E) Since its inception, the OSINT unit has provided OSINT awareness for multiple events, including the 2015 Papal Visit and multiple National Special Security Events (NSSEs), and has currently expanded operations in conjunction with ISD to support the 2016 Presidential Campaign. Currently, OSU is supported with operations mission support funding. This funding stream supports the necessary connections, data sources, and hardware maintenance. The unit has also successfully developed partnerships with National Capitol Region partners, including the US Capitol Police and Washington Fusion Center, along with several state fusion centers for localized support during special events. These partnerships ensure the necessary information sharing relationships are in place to support planned and emerging protective requirements.

BACKGROUND

History of the Program

With the establishment of public email addresses for the President and Vice President in 1993, individuals were able to send threatening correspondence to USSS protectees. The Protective Intelligence and Assessment Division (PID) responded by handling this new threat stream within the existing "region-based" structure. As multi-jurisdictional issues arose due to the subpoena process and the cases became more complex, the PID/Risk Management Branch created the Internet Threat Unit (ITU) and assigned a part-time Special Agent (SA) and one Protective Intelligence Research Specialist (PIRS) to manage these cases exclusively from initial referral to case closure. As the years passed, ITU was supplemented with additional staff, desktop search tools, and advanced training in order to establish a robust element in PID for investigating these types of investigations.

In the fall of 2010, ITU successfully piloted the first open source monitoring effort by reviewing President Obama's public Facebook page for threats and unusual interest statements. Afterwards, ITU operations were supplemented with an open source service contract for searching the open Internet for threatening items of interest. This was done to provide PID with a greater situational awareness of the real-time threat environment. The effect of this proactively searching resulted in a dramatic increase in incident volume, which presented challenges for daily review and incident case management. PID management reviewed mission requirements and isolated searching activities to identifying threats aligned with protectee travel and location. The advance process is referred to "time and place" searching and would allow OSU to better mitigate and manage OSINT requirements.

As these ITU requirements changed and were outside the scope of the original service contract, ITU personnel were trained in advanced operational-based open source intelligence techniques and began to actively support open source intelligence monitoring (OSINT). The newly trained analysts would soon replace the automated searching upon contract termination. It was proved the ITU analysts were more efficient at identifying relevant threats then via a service contract. This was confirmed when PID conducted a comparison of ITU analyst findings versus contractor findings. The results revealed PID analysts held greater familiarity with USSS mission requirements, and as such, could better align OSINT search activities and produce higher quality results. The goal was now to provide the analysts with the most efficient collection tools to assist and streamline their OSINT practices. As the transition occurred, these analysts were assigned to multiple events during the 2012 Presidential Campaign year and coverage was expanded for the White House complex.

PID formally changed the name of the ITU to the Open Source Intelligence Unit (OSU) in March 2014 and became part of the Operations Support Section. At the time, case management activities were moved to the Case Management Section to free up the Open Source Intelligence Unit (OSU) to fully focus on its three primary mission requirements: (1) OSINT monitoring, (2) supporting investigations, and (3) reviewing incoming White House threat correspondence for open source leads. Under this new framework, OSU routinely disseminates OSINT products via bannered products to executive staff (Director and Assistant Directors), protective details, field offices; as well as non-bannered products internally to PID advance personnel, specialty desks, and Foreign Assessment and Counterterrorism Branch staff.

Past successes, such as the support for the 2012 Campaign and its conventions, were followed-up with unprecedented level of support for multiple events in the fall of 2015, to include: the visit of Pope Francis to the United States; the 70th Session of the United Nations General Assembly, and the visit by the President of China.

Existing Status (As Is)

As of fall 2015, OSU has (b)(7)(E) (b)(7)(E) (b)(7)(E) assigned to PID/OSU. PID employees conduct monitoring of the open source environment to identify potential threats and minimize risks directed to Secret Service protectees and protected sites. This capability provides Secret Service operational components near real-time situational awareness of concerning behaviors of interest identified in the open source environment.

The objectives of OSU are stated on the next page.

Open Source Intelligence Unit Core Objectives

- Provide guidance and coordinate open source intelligence research to support protective operations and investigations
- Review and analyze open source information, to include social media networks in real-time, to support protective intelligence advances and investigations
- Provide guidance on subpoena requirements for internet-based investigations
- Coordinate initial investigation of unknown subjects whose location is unknown
- Conduct open source vulnerability assessments for protectees
- Support critical systems protection investigations
- Complete other complex open source and cyber related special projects as requested
- Support Critical Systems Protection (CSP) investigations

To meet the above objectives, OSU relies on software licenses and a high-speed data connection to research and organize publicly available information more effectively. By leveraging this technology, OSU maintains its ability to: a) conduct more effective real-time social media monitoring to capture the digital signatures and geo-location of alleged offenders or potential witnesses; b) provide more timely notification to the protective details and field offices of incidents of immediate concern; and c) allow PID the ability to tailor its monitoring and dissemination efforts to meet the specific needs of major events or protectees by using geospatial software to focus on social media activity in a specified area. An overview of the technology currently leveraged by OSU is below.

In the fall of 2015, the emerging requirement for OSINT support for the 2016 Presidential Campaign presented significant staffing challenges. As noted earlier, internal studies showed the best OSINT analysis is conducted by a trained USSS OSINT analyst – not simply a software solution. In order to resolve this challenge, leadership recommended PID utilize temporarily assigned employees via the Investigative Analyst (IA) Program. The IA personnel have existing skills and abilities similar to PIRSs which enable a fast deployment. The use of the IAs will ensure OSU provides the necessary OSINT support for candidate details in the absence required staffing levels. In November and December 2015, (b)(7)(E) of IAs were trained and deployment to PID began in November 2015. The deployment will continue until Inauguration Day 2017.

Managed Internet Service

Managed internet service provides dedicated internet access service via a leased (b)(7)(E) network line. OSINT monitoring and research requires reliable high speed access to large volumes of data from the Internet. High speed internet access is essential to the OSINT mission to support the overall protective mission of the Secret Service. OSU has been a user of a managed internet service (b)(7)(E) line since FY 2013.

(b)(7)(E)

situational awareness and threats to protectees, protectee sites, and significant events based on geographic location.

Data Subscription

A data subscription provides OSINT analysts with access to large volumes of social media data via real-time data streams for meaningful information related to illicit activity on the open web. This data subscription is used daily by OSU personnel and is essential in the protection of Secret Service protectees by providing awareness of this specialized content for situational awareness and threats to protectees, protectee sites, and significant events based on geographic location. OSU has held a data subscription since FY 2014.

Open Source Intelligence Software

An open source intelligence exploitation software tool is designed to quickly aggregate and standardize information from a wide range of data sources. The software focuses on automating the search, extraction, and organization of multi-source information into standardized data sets for analysis and exploitation by OSNIT monitors. Desktop software is used daily by OSU personnel to assist in the protection of Secret Service protectees by providing awareness of social media content for situational awareness and threats to protectees, protectee sites, and significant events based on geographic location. OSU has been a user of this type of software since FY 2013.

Dark Web Data Subscription

Structured data streams cultivated from the Dark Web allow OSINT monitors to search for meaningful data related to illicit activity not on the open web. This data subscription is used daily by OSU personnel and is essential in the protection of Secret Service protectees by providing awareness of specialized content for situational awareness and threats to protectees and protectee sites. OSU has held this type of subscription since FY 2014.

MISSION NEED STATEMENT

The Secret Service protective mission requires near real-time situational awareness of threats to protectees, protectee sites, and significant events. To meet this need, OSU gathers, analyzes, evaluates and disseminates open source information about individuals, groups, and activities that post a potential threat to persons, facilities, and events protected by the Secret Service. To provide actionable OSINT in support of protective intelligence investigations and protection-related situational awareness, OSU must have the ability to rapidly research and organize publicly available information.

OSU requires technology and highly trained analysts to provide open source support for all protective intelligence advances and investigations, 24/7. The technology must include a dedicated internet access service optical carrier, an (b)(7)(E) renewable data subscription services, and renewable software and software licenses. A full-time program manager is sought to manage the program, document program activities, and identify future enhancement options as industry technologies emerge in the open source arena.

Mission Support Scenario 2

Upon request, OSU will support ongoing protective intelligence investigations with research to identify a person of interest's online footprint, or to identify potential online leads to assist an active investigation to locate and identify a person of interest. As such, the OSINT analyst performs a standard set of searches across multiple open source platforms to identify relevant open source information in social media and other open source sources, and then cross checks it within appropriate public records data bases and internal Secret Service law enforcement databases. Once the analysis is complete, an "Open Source Intelligence Research" product will be produced for dissemination to the customer. Depending on the complexity of the investigation or sensitivity of the circumstances, the product may require multiple levels of supervisory review and dissemination.

These products reflect the open source information available to the analyst at the time of research, and may not be inclusive of all intelligence capabilities outside open source.

It should be noted that under certain circumstances, an OSINT analyst may be providing operational support during trip coverage, but be called up to provide investigative support while supporting this same visit, which reflects a combination of both "Mission Operation" and "Mission Support."

COST, SCHEDULE, AND PROGRAM PERFORMANCE

Program Performance/Metrics

PID developed program performance metrics for OSU to encourage performance improvement, effectiveness, and efficiency. The program performance metrics fall into three main categories: response time, system availability, and productivity.

Response Time is measured by the number of threat notifications or requests received against the time it takes OSU personnel to respond. The key metrics include Mean Response Time in days.

System Availability is measured by the amount of time the OSINT systems are working at full functionality, including data subscriptions, during the time required to do so. The key metrics include Mean Time to Failure and Mean Time to Repair. This would include technical support as required by contract agreements.

Productivity is measured by the number of hours OSU personnel are doing open source monitoring relative to the number of OSU personnel working. The number of PID personnel working on day-to-day monitoring is impacted by variable assignments derived from impacting factors like protectee travel. The

(b)(7)(E)

(b)(7)(E)

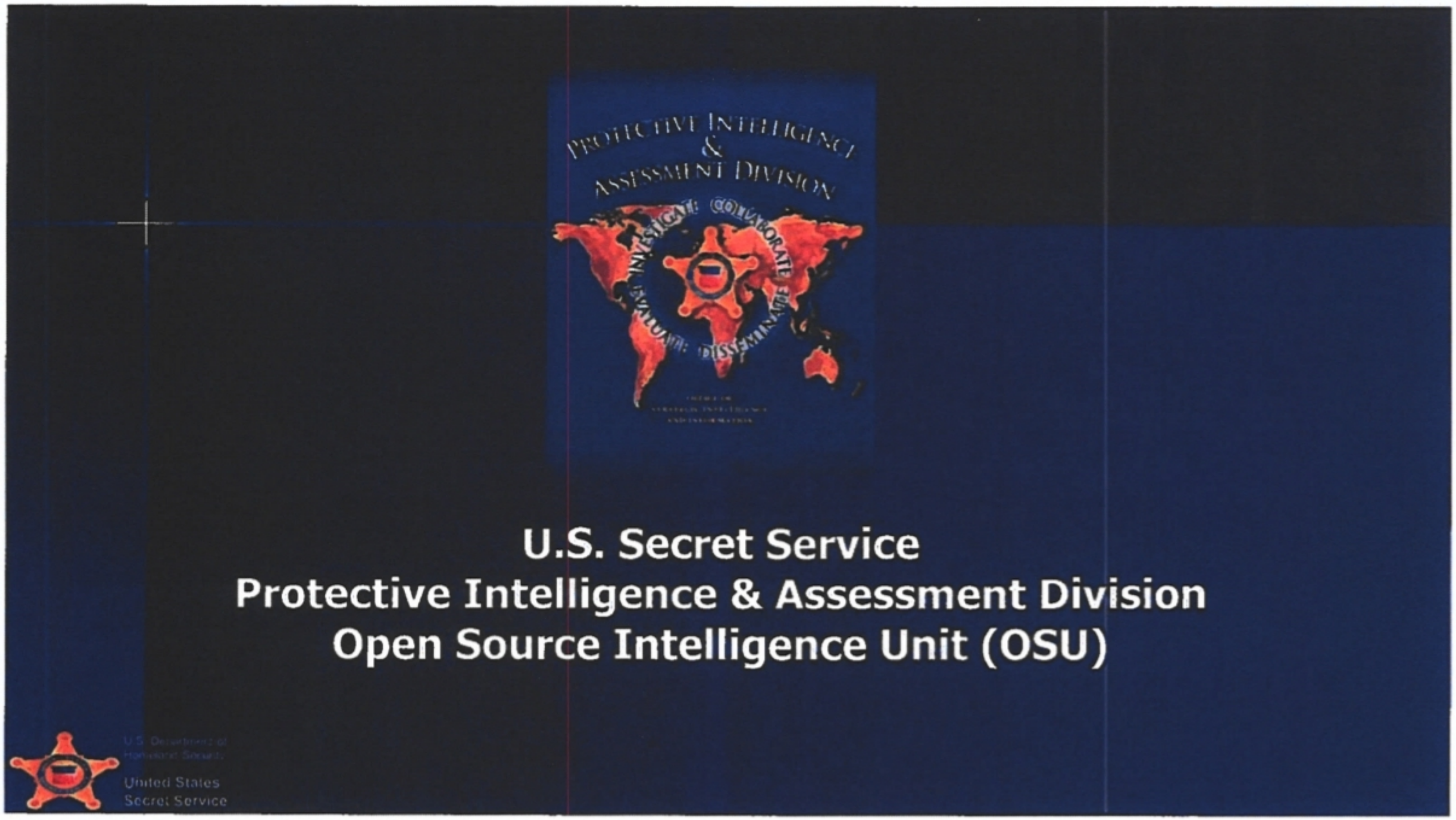
FUTURE INITIATIVES

During FY-16 and continuing into FY-17, OSU will continue to build upon its staffing increases, which will include a minimum of (b)(6);(b)(7)(C to OSU (for a total of 13 PIRSs) to support 24/7/365 coverage, thereby providing the minimum staffing to support activities and reduce overtime costs. Additionally, an increase of supervisory analyst staffing is required to maintain performance oversight and staff leadership.

OSU management will continue to pursue a GS-14 level Program Manager for program management, including acquisition management, technical coordination, and budget tracking. This was initially requested in the FY-17 RAP submission.'

OSU management will continue to recommend and support increasing the SII budget to incorporate a permanent line item for OSU within the base budget.

OSU management will procure the necessary hardware and software to maintain the black line network and work with IRM to sustain the black line virtual network.


PROTECTIVE INTELLIGENCE
&
ASSESSMENT DIVISION
U.S. Secret Service
Protective Intelligence & Assessment Division
Open Source Intelligence Unit (OSU)
United States
Secret Service

What is Open Source Intelligence?

- Open-Source Intelligence (OSINT) is intelligence collected from publicly available sources
- OSINT includes all publicly accessible sources of information, such as-
  - Social media/networking sites
  - News media
  - Public data
- OSINT is defined by the U.S. Director of National Intelligence as, "produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement."

United States Secret Service

Open Source Intelligence (OSINT) Mission

- Responsible for providing OSINT support for
  - Protective Operations / Trip Advances
  - Protective Intelligence Investigations
  - Situational awareness for agency protective & investigative missions
- Conducts research for demonstration activity
  - White House Complex
  - Protectee Sites
  - Activities affecting the National Capital Region
- Creates internal information bulletins on individuals or groups affecting USSS protected interests
- Conducts OSINT research for threats received by the White House Office of Presidential Correspondence

U.S. Department of Homeland Security
United States Secret Service

OSU Members

ATSAIC (b)(6);(b)(7)(C)

SA (b)(6);(b)(7)(C)

SA

SvPIRS (b)(6);(b)(7)(C)

SrPIRS (b)(6);(b)(7)(C)

PIRS

PIRS

PIRS

PIRS

PIRS

PIRS

PIRS

PIRS (b)(6);(b)(7)(C)

U.S. Department of Homeland Security

United States Secret Service

Open Source Intelligence Monitoring

OSINT Monitoring

1. Threat Identification
2. Situational Awareness

OSINT Monitoring Mission is to identify threats and provide situational awareness for Secret Service protective operations

U.S. Department of Homeland Security

United States Secret Service

OSU Requests

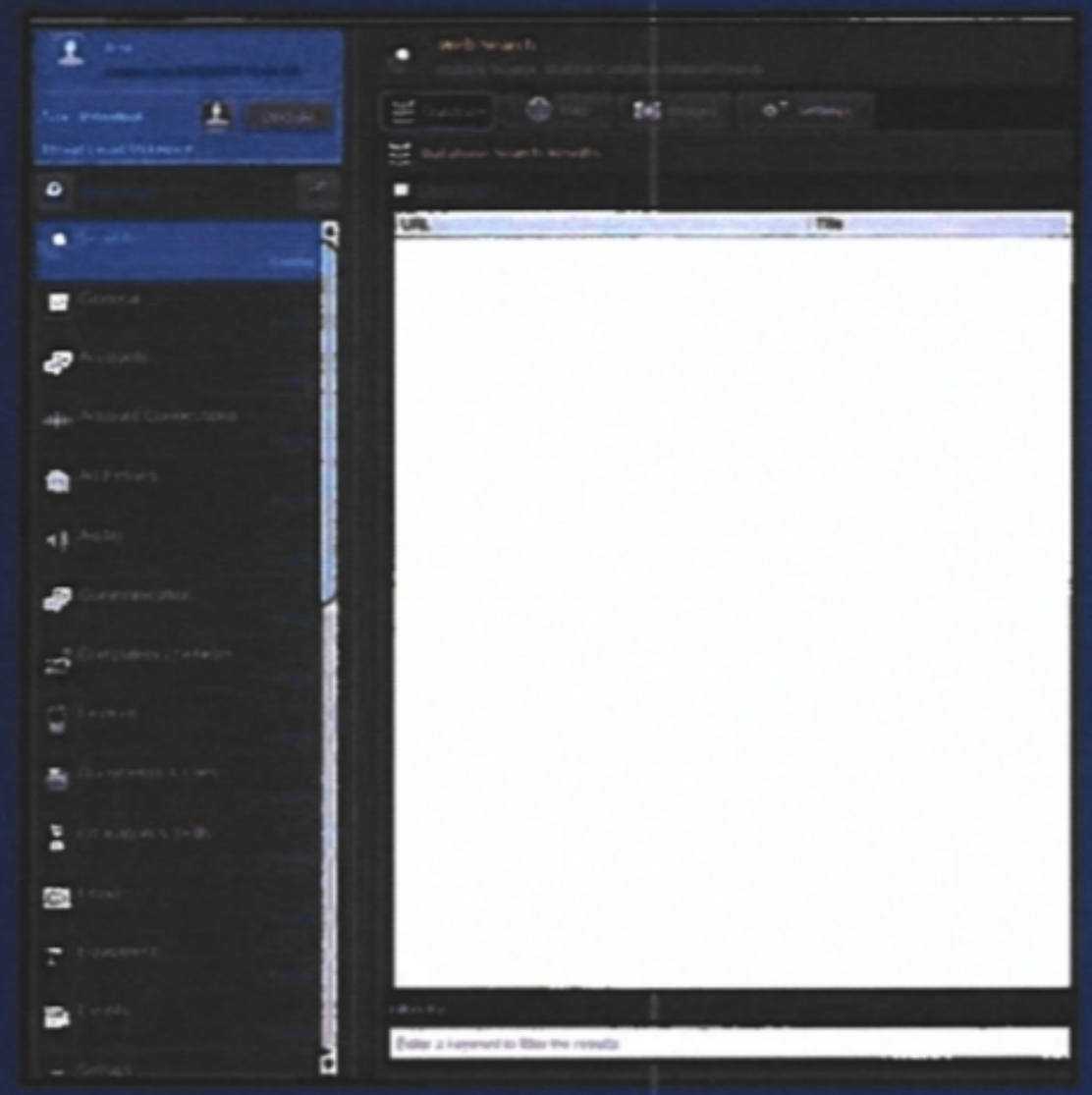
- Demonstration update
- Locate and/or identify potential PI subjects
- Further information on major incidents as news develops

U.S. Department of Homeland Security

United States Secret Service

OpenIO

- AOI Fences
- Keywords
- Entity Extractions



United States
Secret Service

OpenIO:
Situational Awareness - OPSEC

- Photograph discovered in OpenIO while monitoring POTUS' trip to South Africa

- (b)(7)(E)

- Posted by journalist

United States
Secret Service

Demonstrations

- White House Complex, protectee sites, and large events affecting the NCR
- Permit vs. social media postings

United States Secret Service

OSINT Support Operations

- Assessment and sentiment reports
- ECOMMS and Letters forwarded by the White House Office of Presidential Correspondence
- Threatening/inappropriate communications received by protectees
- Discuss incidents routed to OSU
- Double coverage during large events

U.S. Department of Homeland Security
United States Secret Service

White House Emails and Letters

- Monitor forwarded White House ECOMMS/Letters
- In certain cases, OSU will notify the PIOC of any exigent threats

U.S. Department of Homeland Security

United States
Secret Service

Incidents Routed to OSU

- If a request is sent to the PIOC and an appropriate regional jurisdiction could not be determined, the incident will be routed to OSU for further investigation

U.S. Department of Homeland Security

United States Secret Service

Double Coverage

- During major events (i.e NSSEs), double layer coverage may be considered
  - OSU analyst assigned to the PIOC continue normal operations
  - Additional layer with research focused on the event; also coordinates with the PICC if necessary

United States
Secret Service

Questions?

U.S. Department of Homeland Security

United States
Secret Service